IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

(Attorney Docket № 14182US02)

In the Application of:

Ed H. Frank, et al.

Serial No. 10/658,139

Filed: September 9, 2003

For: METHOD AND SYSTEM FOR PROVIDING SEAMLESS CONNECTIVITY AND COMMUNICATION IN A MULTI-BAND MULTI-PROTOCOL HYBRID WIRED/WIRELESS NETWORK

Examiner: Hieu T. Hoang

Group Art Unit: 2152

Confirmation No. 3006

Electronically Filed on July 3, 2008

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The Applicant requests review of the final rejection in the above-identified application, stated in the final Office Action mailed on April 3, 2008 (hereinafter, the Final Office Action) with a period of reply through July 3, 2008. The Applicant also requests review of the arguments stated on pages 2-3 of the Advisory Office Action mailed on May 19, 2008 (hereinafter, the Advisory Office Action). No amendments are being filed with this request.

This request is being filed with a Notice of Appeal. The review is being requested for the reasons stated on the attached sheets.

REMARKS

The present application includes pending claims 1-31, all of which have been rejected. Claims 11-20 have been rejected under 35 U.S.C. § 101 as being non-statutory because the claimed invention is allegedly directed to non-statutory subject matter. Claims 1-7, 9-17, and 29-31 are rejected under 35 U.S.C. § 102(e) as being anticipated by Ala-Laurila et al. (US 6,587,680, hereinafter "Laurila"). Claims 8, 18, and 28 are rejected under 35 U.S.C. § 103(a) as being anticipated over Laurila in view of Bhagwat et al. (US 6,651,105, hereinafter "Bhagwat").

The Applicant respectfully submits that claims 1-31 define patentable subject matter in view of the following remarks and arguments.

I. REJECTION OF CLAIMS 11-20 UNDER 35 U.S.C. § 101

The Applicant maintains the arguments stated in pages 12-14 of the May 5, 2008 response regarding the rejection of claims 11-20 under 35 U.S.C. § 101. More specifically, **the May 5, 2008 response provided explicit citations from the MPEP, where "computer-readable medium" is deemed statutory without any additional requirement for further defining what "computer-readable medium" is.** In page 2 of the Advisory Office Action, the Examiner has adopted an overly broad and unreasonable interpretation, alleging that "computer-readable medium" reads on any transmission media, signals or signal-carrying waves. The Applicant respectfully disagrees. The Examiner is reminded that the term "medium" has a very specific meaning in the art, which is different than Examiner's overly-broad interpretation. For example, the Examiner is referred to "The Authoritative Dictionary of IEEE Standards Terms," 7th Edition, page 683, where the term *"medium"* is defined as "the material, or configuration thereof, on which data are recorded; for example, paper tape, cards, magnetic tape." In other words, "medium" is a physical material used for storing of data. The Applicant maintains that the rejection under 35 U.S.C. § 101 should be withdrawn and claims 11-20 should be allowed.

II. REJECTION UNDER 35 U.S.C. § 102

The Applicant turns to the rejection of claims 1-7, 9-17, 19-27, and 29-31 under 35 U.S.C. § 102(e) as being anticipated by Laurila. Without conceding that Laurila qualifies as prior art under 35 U.S.C. 102(e), the Applicant respectfully traverses this rejection as follows.

In page 2 of the Advisory Office Action, the Examiner states: "SA is transferred between various APs to avoid the need for *a new authentication key that is used to authenticate both ends of the communications pair* that is made up of a mobile terminal and an AP

(Laurila, col. 5, lines 43-50)." The Applicant respectfully disagrees. Laurila, at col. 5, lines 43-50, states the following:

> An authentication key for both ends of the communication pair that is made up of a mobile terminal and an AP is originally generated by a scaleable key management protocol, for example Internet Key Exchange (IKE). Security associations are transferred between the various APs that are within the wireless communication system in order to avoid the need for a new and different key exchange during each handover.

As clearly seen from the above citation, **Laurila at col. 5, lines 43-50 (or any of the remaining portions), does not disclose that the authentication key "is used to authenticate both ends of the communications pair," as alleged by the Examiner.**

As explained in the May 5, 2008 response, Laurila's security associations (SAs) involve the transfer of security keys, which are simply used for encoding and decoding of the data. Obviously, the security keys are not used in any way for purposes of authenticating of one device by another. As explained in the May 5, 2008 response, Laurila has provided for a separate procedure for authenticating of one device by another. Namely, Laurila uses the challenge/response sequence for purposes of authentication, which is separate from the transfer of the SA.

With regard to the rejection of independent claim 1 under 102(e), the Applicant submits that Laurila does not disclose or suggest at least the limitation of "providing authentication information related to said initial authentication to at least one of a second access point and a third access point," as recited in claim 1 by the Applicant.

In page 4 of the Final Office Action, the Examiner seems to equate Laurila's disclosure of the security association (SA) to the Applicant's "initial authentication," as recited in claim 1. The Applicant respectfully disagrees and points out that Laurila's "security function" and "authentication" are two separate and distinct functions. For example, as explained herein below, Laurila's mobile terminal MT 12 (asserted as an access device by the Examiner) and the new access point AP_new 114 are each separately and independently authenticated through a procedure of generating challenges and comparing the calculated response with the correct response. There is no Security Association (SA) parameter involved in the authentication procedure. In other words, the SA parameter exchange procedure is separate and independent of the authentication procedure using challenges and responses.

The Applicant points out that Laurila, at col. 8 lines 2-6, clearly discloses that the SA utilizes a common set of keys, which are necessary to achieve security function(s). Laurila, at col. 8 lines 6-16, discloses that instead of using SA for authentication procedure in the mobile terminal MT 12 and in the AP_new 114, as asserted by the Examiner, Laurila discloses that the transfer of SA is for eliminating the use of public key encryption (for security) and for minimizing the additional messages needed (message encryption and decryption). Laurila discloses the benefits of transferring SA,

namely, to minimize delays in services such as VOIP and video distribution. **In other words, Laurila discloses that the SA parameter is retrieved and transferred for the purpose of minimizing the need of exchanging security messages that would otherwise cause undesirable delays in certain types of services. There is no disclosure or suggestion by Laurila that the SA is utilized as information to facilitate authentication in the MT 12 and the AP_new 114.**

Therefore, the Applicant maintains that Laurila does not disclose or suggest that "the SA is stored and read as authentication information, retrieved from AP_old," as asserted by the Examiner.

The Examiner is further referred to Laurila at col. 8 lines 23-34, where Laurila discloses that the generation of challenges and calculating of responses between the MT 12 and the AP_new 114 are separated from the SA. Laurila also discloses that new authentication is required for the mobile terminal 12 moving from cell 18 (form AP_old 14, asserted as the first access point by the Examiner) to the new cell 118 (to AP_new 114, asserted as the second access point by the Examiner) through a series of challenge and response procedure (ap_response, mt_response and ap_challenge, mt_challenge), which are separate and unrelated to the SA parameters.

For example, Fig. 2 and col. 8 lines 42-48 of Laurila discloses that the mobile terminal MT 12 generates a challenge (mt_challenge) and is sent as a message MAC_REASSOCIATE_REQ to the AP_new 114. The AP_new 114 sends back a reply message MAC_AUTHENTICATE_REQ with a generated challenge (ap_challenge) and a calculated response (ap_response). The MT 12 performs an authentication (AP Authentication) by comparing the ap_response with the correct response. The MT 12 replies with a message MAC_AUTHENTICATE_RESP carrying a response (mt_response) to the AP_new 114. The AP_new 114 performs an authentication (MT Authentication) by comparing the mt_response to the correct response. Upon successful authentication, the AP_new 114 returns a message MAC_REASSOCIATE_RESP to confirm successful handover so that the payload traffic can be resumed (see Laurial in Fig. 2). **The Applicant points out that no SA information is used in any of the authentication messages throughout the entire authentication process.** Similar processing is disclosed with regard to Laurila's FIG. 3.

To summarize the above arguments, Laurila discloses that the SA parameters are for security information sharing during connection process when the MT 12 is moved from an AP_old 14 to an AP_new 114 to minimize interruptions caused by additional security messages. Laurila discloses that an authentication procedure is required in the hand over process, and the SA exchange is unrelated in any way to Laurila's authentication procedure.

Based on at least the foregoing, the Applicant maintains that the SA parameter exchange is not "initial authentication," as asserted by the Examiner. Therefore, Laurila does not disclose or suggest "**providing** authentication information related to said **initial authentication to** at least one of a second access point and a third access point," as recited in claim 1 by the Applicant. With regard to the rejection of independent claim 1 under 102(e), the Applicant further submits that Laurila does not

disclose or suggest at least the limitation of "**servicing** said access device by one of said first access point, said second access point and said third access point **based on said initial authentication**," as recited in claim 1 by the Applicant.

Based on the foregoing arguments that the SA is not disclosed or suggested as "initial authentication" by Laurila, and new authentications are required by both the mobile terminal MT 12 and the AP_new 114 during the handover, subsequently, the Applicant maintains that Laurila does not disclose or suggest "**servicing** said access device by one of said first access point, said second access point and said third access point **based on said initial authentication,**" as recited in claim 1 by the Applicant.

Accordingly, the Applicant respectfully submits that claim 1 is not anticipated by Laurila, and therefore is allowable. The Applicant respectfully requests that the rejection of claim 1 under 35 U.S.C. § 102(e) be withdrawn. Independent claims 11 and 21 are similar in many respects to independent claim 1. Therefore, the Applicant respectfully submits that claims 11 and 21 are also allowable at least for the reasons stated above with regard to claim 1, and respectfully requests that the rejection of claims 1, 11 and 21 under 35 U.S.C. § 102(e) be withdrawn. The Applicant also maintains the arguments stated in pages 23-30 of the May 5, 2008 response regarding the allowability of the dependent claims.

III. Conclusion

The Applicant respectfully submits that claims 1-31 of the present application should be in condition for allowance at least for the reasons discussed above and request that the outstanding rejections be reconsidered and withdrawn. The Commissioner is authorized to charge any necessary fees or credit any overpayment to the Deposit Account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: July 3, 2008

By: /Ognyan Beremski/
Ognyan Beremski, Reg. No. 51,458
Attorney for Applicant

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
Telephone: (312) 775-8000
Facsimile: (312) 775 – 8100

(OIB)